Minutes of the 9 December 2008 Meeting

USPS, 475 L'Enfant Plaza, SW, Washington, DC
Conference Room 2P316

A. AGENDA

1. Welcome / Introductions
2. Discussion on 12 November 2008 FPKIPA Minutes
3. Results of the e-vote on the VeriSign WTCA Audit and Audit Letter
4. PK-Enabling
5. FPKI Certificate Policy Working Group (CPWG) Report
6. FPKI Management Authority (FPKI MA) Report
7. FPKIPA FY08 Year-End Accomplishments
8. Adobe White List Initiative
9. Federal Agency Use of SSPs
10. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 12/15 (or 80%) where a two-thirds majority was required.

We redacted contact information in the published FPKIPA minutes at the request of FPKIPA members. This information will be posted to a secure web site for FPKIPA members only at some point in the future. FPKIPA minutes already posted on the website have been redacted to remove POC information. FPKIPA members needing POC information on other members and participants should contact the Secretariat at Judith.fincher@pgs.protiviti.com.

Organization	Name	Telephone
Department of Commerce (NIST)	ABSENT	
Department of Defense	Mitchell, Debbie	Teleconference
Department of Health & Human Services	Slusher, Toby	Teleconference
Department of Homeland Security	Hagerling, Don /Tanyette Miller	
Department of Justice	Morrison, Scott	
Department of State	McCloy, Mark	
Department of Treasury	Jim Schminky	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Hannan John	
GSA	Spencer, Judith	
NASA	Levine, Susan	Teleconference

Organization	Name	Telephone
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	ABSENT	
USPS	Stepongzi, Mark	
USPTO	ABSENT	

OBSERVERS

Organization	Name	Telephone
KPMG	Faut, Nathan	
IdenTrust	Schambach, Marco	Teleconference
FICC/FPKIPA Support (Contractor, FC Business Systems, LLC)	Petrick, Brant	
Executive Office of the President (EOP)	Smith, Winsfield	
Department of State/ Co-chair, CPWG (Contractor, ManTech)	Froehlich, Charles	
Wells Fargo	Drucker, Peri	Teleconference
State of Illinois	Anderson, Mark	Teleconference
eValid8	Dilley, Brian	
FPKI MA Technical Lead (Contractor, Protiviti Government Services)	Brown, Wendy	
FPKIPA Support/Secretariat (Contractor, Protiviti Government Services)	Fincher, Judy	
FPKIPA Support, Co-Chair CPWG (Contractor, Protiviti Government Services)	McBride, Terry	
Cipher Solutions, Inc.	Ahuja, Vijay	
DoE	Dan Lonnerdal	
DoE	Varghese, Jebby	

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Judith Spencer, Interim Chair

The FPKIPA met at the USPS Headquarters Building located at 475 L'Enfant Plaza, SW, Washington, DC, in Conference Room 2P316. Judith Spencer, Interim Chair, called the meeting to order at 9:44 a.m. and conducted introductions of those present in person and via teleconference. We wish to thank Mark Stepongzi of the USPS for hosting the meeting and holiday party and the other members of the FPKIPA for bringing food/drink and party supplies.

Agenda Item 2

Discussion on 12 November 2008 FPKIPA Minutes— Judy Fincher

Because the 12 November 2008 minutes were delayed by the birth of Terry McBride's baby boy, we will vote on the minutes at the January 2009 FPKIPA meeting.

Agenda Item 3

Results of the e-vote on VeriSign WTCA Audit and Audit Letter—Judy Fincher

Ms. Fincher reported that 13 agencies voted to approve the VeriSign WTCA Audit and Audit Letter, or 86.7% where a 75% majority vote was required. Commerce and Treasury did not vote.

Agenda Item 4

PK-Enabling—Judith Spencer, Debbie Mitchell

Ms. Spencer reported on a meeting she held with Debbie Mitchell and the NSA folks two weeks ago to discuss setting up a work team to capture "lessons learned" on PK-enabling. Ms. Mitchell said that Carrie Webster of DISA is responsible for PK-enabling for DoD and would make a presentation at the January 2009 FPKIPA meeting on that topic.

Agenda Item 5

FPKI Certificate Policy Working Group (CPWG) Report—Charles Froehlich, Judith Spencer

a) **VeriSign Status Update**
Charles Froehlich and Ms. Spencer reported on the status of the VeriSign Cross-Certification process. Mr. Froehlich said the Operational Parameters Review is incomplete and the interoperability (directory) testing is underway. Nick Piazzola also owes the CPWG a response to our comments. Ms. Spencer hopes these issues can be resolved in time for an e-vote on the VeriSign Cross-Certification the week of January 5, 2009.

b) **Verizon Business Status Update**
The CPWG completed the Verizon Business mapping and sent our comments to Debb Blanchard. She is also reluctant to accept the FPKIPA policy that "high" is reserved for the FPKIPA and wants to be cross-certified at "high" in order to service the local, state and tribal governments.

Ms. Spencer said that to achieve PIV interoperability, external entities such as VeriSign non-Federal SSP and Verizon Business non-Federal SSP, need to cross certify at Medium Hardware in order to issue PIV-interoperable cards with PKI certs to the FRAC, TWIC, and SWAC communities. SWAC is the Secure Worker Access Consortium—for port authorities. She said she expects the FICC to approve the White Paper on PIV Interoperability for non-Feds at its Thursday meeting.

c) State of Illinois Mapping
Mr. Froehlich said that the CPWG completed the mapping matrices of the State of Illinois (General, Medium Hardware, and the "deltas" for Medium and Basic). The CPWG sent back to Illinois questions on several unresolved items. Hopefully, these can be resolved at the 16 December 2008 CPWG meeting. At that meeting, the CPWG will also review the "white space" mapping, e.g., unmapped sections of the Illinois CP.

d) DoD Change Proposal: FBCA CP Change Proposal: 2008-xx
Ms. Mitchell has introduced a FBCA CP Change Proposal to eliminate the in-person antecedent for Medium Hardware. Ms. Spencer said this request requires discussion and that the CPWG would examine this change proposal at its 16 December 2008 meeting.

e) DoD Change Proposal: Common Policy Framework CP Change Proposal: 2008-xx
This Change Proposal would relax the next update period—currently 18 hours-- for Common. Both DoD and the DoS have operational issues: their overseas CAs are not able to pull down the new CRLs in time to meet the current deadline. The proposal is to extend the next update period, but the revised next update period has been "left open," i.e., there is no recommendation in the Change Proposal. The CPWG will also examine this Change Proposal at its 16 December 2008 meeting.

Agenda Item 6

FPKI Management Authority (FPKI MA) Report—Wendy Brown, Judith Spencer

Wendy Brown said that the directory performance has improved over the past two weeks and that implementation of the Directory Improvement Strategy Plan will lead to more improvements over the next few months. In addition, the FPKI MA will set up a Technical Advisory Board to help guide the strategic direction of the FPKIPA on issues such as the SIA extension, she said.

The FPKI MA issued cross-certificates to Wells Fargo and the Department of State last month.

Ms. Spencer said that the FPKI MA would relocate physically in the near future—both the Primary and Secondary sites. Although we are in the midst of a technology refresh, we intend to handle the transition with as little disruption as possible.

Agenda Item 7

FPKIPA FY 08 Year End Accomplishments—Judith Spencer

Ms. Spencer read from the FPKIPA FY08 Year End Accomplishments document prepared by Judy Fincher. This report also included events and accomplishments performed from January through December of CY 2008.This report will be distributed to the FPKIPA listserv soon. Highlights included:

(1) The FPKIPA cross-certified with a second PKI Bridge (Safe Bio-Pharma) in FY 2008. It also cross-certified with new PKIs at the Department of State, Wells Fargo, and DoD and added a cross-certification with the Department of the Treasury, USPS and GPO at Medium Hardware. Several agencies either cross certified at Medium Hardware and/or upgraded to that Level of Assurance, using the 3647 RFC format. FY08 also saw an

influx of outsourced PKIs utilizing the services of SSPs and the GSA Managed Service Offering (MSO), as Federal Agencies began to comply with HSPD-12/FIPS 201.

(2) Three existing cross-certified members (HHS, NASA and DHS) decommissioned their PKIs and sought the services of an SSP in FY08.

(3) In July 2008 MIT Lincoln Laboratory notified the FPKIPA that is was no longer able to maintain the relationship with the FBCA and was terminating the relationship. The FPKIPA complied with this request and revoked the cross-certificate in July 2008.

(4) The Certificate Policy Working Group (CPWG) edited the FBCA and C4CA *Criteria and Methodology* document.

(5) The FPKIPA co-sponsored with NIST, OASIS, and Internet2, the 7th Symposium on Identity and Trust on the Internet (IDtrust 2008) conference held at NIST in March 4-6, 2008. The 8th Symposium on Identity and Trust on the Internet (IDtrust 2009) will be held April 14-16, 2009 at NIST.

(6) The CPWG updated the mapping of the FBCA CP and Common Policy Framework CP to NIST SP 800-53A.

(7) Dr. Peter Alterman was appointed Deputy Associate Administrator (DAA) for the Office of Technology Strategy, Office of Governmentwide Policy/GSA on 16 July 2008.

(8) Judith Spencer replaced Dr. Alterman as the Interim Chair of the FPKI Policy Authority,

(9) The CPWG processed six (6) FBCA CP Change Proposals and two (2) Common Policy Framework CP Change Proposals.

(10) Three members of the Four Bridge Forum (4BF) signed an Agreement to Cooperate in October2008 (CertiPath, SAFE Bio-Pharma and FBCA).

(11) The CPWG performed seven (7) Policy Mappings and "White space" mappings for entities wishing to be cross certified with the FBCA, as well as Operational Parameters Reviews.

Action Item 8

Adobe White List Initiative—Judith Spencer, John Hannan

Ms. Spencer described the efforts underway to get the Common Policy root into the Adobe Trust List Store and thanked John Hannan for his role in making this happen. We have submitted an official application and the next step is an agreement in the April timeframe.
.

Agenda Item 9

Federal Agency Use of SSPs—Judith Spencer, Debbie Mitchell

Ms. Spencer mentioned that there is some concern that we are not tracking which agencies are using which SSPs. "Should we publish this information to the website?" she asked. The views of the FPKIPA were mixed, with some agencies advocating we should do so, notably NRC and DoD. DoD was concerned that there might be players in the trust chain that they would choose not to trust. Ms. Spencer said all SSPs should be trusted equally. In conclusion, Ms. Spencer said that every Federal Agency is issuing PIV cards with digital credentials. Seventy (70) agencies are receiving services from the GSA MSO (running Entrust), she said. She listed other agencies that have signed up with other SSPs: Labor (ORC); EOP (Verizon Business); and NRC (VeriSign).

The memo, "Implementing HSPD-12 using Legacy PKI certificates," is attached.

Agenda Item 10

Adjourn Meeting
Ms. Spencer adjourned the meeting at 10:35 a.m.

CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
285	Judith Spencer and DoD will go off-line to discuss name uniqueness. She suspects there is name collision.	Judith Spencer, Debbie Mitchell	8 May 2007	22 May 2007	Open
315	Dr. Alterman and John Cornell will incorporate language into the FPKIPA audit Cook Book. This language was provided by Noel Nazario of KPMG and says that if customers set up the terms of their Web Trust audits appropriately, the Web Trust audit would satisfy all our requirements.	Dr. Alterman, John Cornell	9 Oct. 2007	13 Nov. 2007	Open
316	Judith Spencer said we should post an explanation of the purpose of the C4CP to the FPKIPA website, explaining that the FPKIPA needs this policy for those entities who cannot meet Federal Bridge cross-certification requirements, but who need an E-Authentication Level 2 credential.	??	13 Nov. 2007	26 Nov. 2007	Open
327	Cheryl Jenkins will send the annotated Implementation Plan to Judy Fincher for distribution to all cross-certified members of the FPKIPA.	Cheryl Jenkins	11 Dec. 2007	January 2008	Open

No.	Action Statement	POC	Start Date	Target Date	Status
331	Dr. Alterman will draft language for the FBCA policy change procedure to do some “reality testing” and distribute it to the FPKIPA.	Dr. Peter Alterman	8 April 2008	13 May 2008	Open
366	Debbie Mitchell will share the finalized DoD Test Plan; the FPKIPA will then review it and decide what pieces they can and cannot do. Then Cheryl Jenkins will follow up to make sure the test plan includes testing at the application level,--not just the PKI level.	Debbie Mitchell, FPKIPA, Cheryl Jenkins	13 May 2008	10 June 2008	Open
371	Dr. Alterman will inform Verizon Business Systems (VBS) that their application was approved and will ask for the ETA for the Policy.	Dr. Peter Alterman	8 July 2008	15 July 2008	Open
373	Deborah Gallagher will check with DHS to verify the FRAC requirement.	Deborah Gallagher	9 Sept. 2008	14 Oct. 2008	Open
375	The FPKIPA Chair will take the enduring proxy and meeting schedule issues under advisement and will notify non-attendees that they risk losing their voting privileges if they persist in unexplained absences and do not designate a proxy when they cannot attend.	Judith Spencer	14 October 2008	12 November 2008	Open

MEMORANDUM FOR FEDERAL AGENCY LEGACY PKIs

SUBJECT: Implementing HSPD-12 using Legacy PKI certificates

[DATE: 10/7/07]

Section 5.4.4 of FIPS 201 states: "Departments and agencies whose PKIs have cross-certified with the Federal Bridge CA (FBCA) at Medium-HW, or High Assurance Level may continue to assert department or agency-specific policy Object Identifiers (OID). Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or id-CommonAuth policy OIDs. (Departments and agencies may continue to assert department or agency-specific policy OIDs in addition to the id-CommonHW and id-CommonAuth policy OIDs in certificates issued after January 1, 2008.)"
In order to facilitate Federal Legacy PKI compliance with this requirement, the Common Policy has been modified to include provisions that exclusively pertain to the Federal Legacy PKIs. By adding language pertaining to naming conventions and off-line root CAs, the main obstacles to compliance with the Common Policy by Federal Legacy PKI agencies have been removed. This should enable the Federal Legacy PKI agencies to express Common Policy OIDs in the PIV Authentication Certificates, as is required to meet the requirements of FIPS 201 (additional certificates for signing and key management can continue to only assert agency OIDs). However, those agencies planning to take advantage of this new language must ensure that they implement their certificates in a manner consistent with other provisions in the Common Policy. A Federal Legacy PKI will be deemed to be issuing PIV Authentication certificates in conformance with the Common Policy if it issues those certificates in accordance with the requirements of a certificate policy that has been mapped to the FBCA CP at the Medium Hardware or High assurance level and in accordance with the following additional provisions that affect certificate issuance:

- Identity proofing requirements (FIPS 201 Section 2)
- 18 hour CRL requirement (FIPS 201 Section 5.4.3) and the requirement to populate the nextUpdate field in CRLs as specified in the Common Policy, section 4.9.7.
- OCSP Requirement (FIPS 201 Sections 5.3 and 5.4)
- Requirement to issue the certificates in conformance with Worksheet 9 of the *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP)* Program [SSP-PROF] (FIPS 201 Section 5.4.2.1).

- Requirement not to post PIV Authentication certificates to a public directory. (FIPS 201 Section 5.4.5.1)

- Requirement to make directory information available via LDAP and HTTP. (FIPS 201 Section 5.4.5.1

Peter Alterman, Ph.D.
Chair